UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
- - - - - - - - - - - - - - - - - -X

UNITED STATES OF AMERICA, :

-v.- : 10 Cr. 96 (DLC)

SERGEY ALEYNIKOV, :

Defendant. :

- - - - - - - - - - - - - - - - - -X

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO DISMISS

PREET BHARARA
United States Attorney for the Southern District of New York, Attorney for United States of America.

JOSEPH P. FACCIPONTI
REBECCA A. ROHR
Assistant United States Attorneys, Of Counsel.

TABLE OF CONTENTS

Table of Authorities

CASES

FEDERAL STATUTES

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
- - - - - - - - - - - - - - - - - -X

UNITED STATES OF AMERICA, :

-v.- : 10 Cr. 96 (DLC)

SERGEY ALEYNIKOV, :

Defendant. :

- - - - - - - - - - - - - - - - - -X

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO DISMISS

The Government respectfully submits this response in opposition to the defendant's motion, dated July 16, 2010 and made pursuant to Federal Rule of Criminal Procedure 12(b)(3)(B) ("Defendant's Motion"), to dismiss Indictment 10 Cr. 96 (DLC) (the "Indictment") on the ground that each of the Indictment's three Counts fails to state a claim. For the reasons stated below, the Government respectfully requests that the Court deny the Defendant's Motion in its entirety.

The Government joins in the defendant's request for oral argument on the motion.

STATEMENT OF FACTS

Because the defendant asserts that the Indictment fails to state a claim on all of its Counts, the Government reviews the Indictment's factual allegations below, as well as relevant facts from the record and facts proffered here that the Government expects to prove at trial.

A. Summary of the Offense Conduct

The Indictment alleges that the defendant stole valuable trade secrets from his former employer, Goldman Sachs & Co. ("Goldman"), with the intent to use those trade secrets for the defendant's own benefit and for the benefit of his new employer, Teza Technologies LLC ("Teza"). Specifically, the Indictment alleges that on June 5, 2009 – the defendant's very last day of work at Goldman – the defendant, without authorization from Goldman and in violation of Goldman's polices on confidentiality, copied, encrypted, and transferred to a computer server outside of Goldman's computer network hundreds of thousands of lines of computer source code. Contained within the source code stolen by the defendant were trade secrets belonging to Goldman and related to Goldman's high-frequency trading business. After the defendant stole the source code, he deleted evidence of his theft from Goldman's computer system.

Nearly a month later, on July 2, 2009, the defendant traveled to the Chicago offices of Teza, a startup company that

was looking to develop its own high-frequency trading business. On that trip, the defendant carried with him a copy of the source code that he had stolen from Goldman.

B. Goldman Sachs & Co. and Teza Technologies LLC

As alleged in the Indictment, Goldman is a company headquartered in New York, New York that provides financial services in the United States and around the world. (Ind. ¶ 1).[1] Like various other financial institutions, Goldman engages in what is commonly known as "high-frequency trading." (Ind. ¶¶ 1, 4). Teza is a startup company that is headquartered in Chicago, Illinois and was founded in early 2009 with the goal of developing its own high-frequency trading business. (Ind. ¶ 2).

C. Goldman's High-Frequency Trading System

High-frequency trading occurs on various financial markets, including national securities markets such as the New York Stock Exchange ("NYSE") and the NASDAQ Stock Market, as well as commodities markets. (Ind. ¶ 4). Companies engaged in high-frequency trading, like Goldman, use sophisticated computer systems to execute scores of trades in short periods of time based upon mathematical formulas that evaluate moment-to-moment developments in the markets and data regarding past trades.

[1]As used herein, "Ind." refers to Indictment 10 Cr. 96 (DLC); "Compl." refers to Complaint 09 Mag. 1553, dated July 4, 2009 and attached hereto as Exhibit A; "Mem." refers to the Memorandum of Law in Support of the Defendant's Motion to Dismiss the Indictment, dated July 16, 2010.

(*Id*.).

As alleged in the Indictment, Goldman's high-frequency trading system has two major components. On the one hand, there are the mathematical formulas, or algorithms, that make trading decisions. (Ind. ¶¶ 4-5). On the other hand, there is the "Platform," a series of computer programs that obtains and processes the latest market data – so that it can be analyzed by the algorithms – and then executes the algorithms' trading decisions. (*Id*. ¶ 5). The Platform's speed in performing these tasks gives Goldman a competitive advantage in its trades. (*Id*.). Goldman makes many millions of dollars in profits from high-frequency trading. (*Id.*)

Although Goldman does not license, sell, or distribute either its trading algorithms or the Platform to other financial institutions or to the general public, Goldman acquired portions of its high-frequency trading system when it purchased the Hull Trading Company for approximately $500 million in or about 1999. (Ind. ¶ 6). Since this acquisition, Goldman has employed many computer programmers to develop and maintain both the Platform and the trading algorithms. (*Id*.).

Goldman takes a variety of measures to protect the confidentiality of its high-frequency trading system. (Ind. ¶ 8). These include, among other things, requiring Goldman employees to enter into a confidentiality agreement and by

blocking and monitoring of certain transfers of data outside of Goldman's computer system. (*Id*.).

D. The Defendant's Theft of Goldman's Trade Secrets

From May 2007 through June 2009, the defendant, a computer programmer, was employed by Goldman as a "vice president" responsible for developing and improving certain aspects of the Platform. (Ind. ¶ 9). At the time he left Goldman, the defendant's total annual compensation was $400,000. (*Id*. ¶ 11). In or about April 2009, the defendant accepted an employment offer from Teza, where his title would be "executive vice president" for "platform engineering," and where he would be responsible for developing Teza's own high-frequency trading business. (*Id*. ¶ 10). At Teza, the defendant would receive an annual compensation package of nearly $1,200,000 – a threefold increase over his compensation at Goldman – which included an annual salary of $300,000 and a guaranteed cash bonus of $700,000 in addition to other compensation. (*Id*. ¶¶ 10-11).

The defendant's last day at Goldman's offices was June 5, 2009. (Ind. ¶ 12). At approximately 5:20 p.m. that day, the defendant uploaded, without authorization, hundreds of thousands of lines of source code for Goldman's high-frequency trading system – including source code for both the Platform and the trading algorithms – to a server outside of Goldman's computer network. (*Id*. ¶ 12).

In doing so, the defendant used a program that he had written for the specific purpose of aiding in his theft of the code. That program copied and compressed certain files of the source code for Goldman's high-frequency trading system. (*Id*. ¶ 12(a)). After copying and compressing the files, the defendant used another program to encrypt them, and thereafter uploaded the compressed and encrypted files to a computer server in Germany, outside of Goldman's computer network. (*Id*. ¶ 12(b)). The defendant's last step was to erase records of this transfer, including the encryption program and encryption key, thereby hiding the fact that he had copied, encrypted, and transferred proprietary Goldman files out of Goldman's computer system. (*Id*. ¶ 12(c)).

The defendant's transfer of source code to the server in Germany was not authorized by Goldman and was in violation of Goldman's policies. (Ind. ¶ 12(b)). After returning to his home on the evening of June 5, 2009, the defendant downloaded the stolen source code from the server in Germany to his home computer, and thereafter copied some of those files to other computers and devices. (*Id*. ¶ 13).

As alleged in the Indictment, this was not the first time the defendant had taken proprietary information from Goldman. (Ind. ¶ 14). In fact, on many occasions throughout his employment at Goldman, the defendant transferred, without

authorization from Goldman and in violation of Goldman's policies, source code for Goldman's high-frequency trading system to his home computers, using methods such as the server in Germany, e-mails sent from the defendant's Goldman e-mail account to the defendant's personal e-mail account, and by copying the code to a portable media player. (*Id*.).

After leaving Goldman, the defendant did not return any of the stolen source code to Goldman, as he was required by Goldman's policies. (Ind. ¶ 14).

On July 2, 2009, the defendant flew from New Jersey to Chicago, Illinois, to attend a meeting at Teza's offices, carrying with him copies of the source code for Goldman's high-frequency trading system, including some of the files the defendant stole on June 5, 2009. (Ind. ¶ 15).

E. <u>The Defendant's Arrest</u>

On July 3, 2009, as he was returning from Chicago, the defendant was arrested at Newark airport in New Jersey by agents with the Federal Bureau of Investigation ("FBI"). After his arrest, the defendant waived his *Miranda* rights and made oral and written statements to the FBI agents, in which the defendant admitted that he had uploaded files from Goldman's computer system on June 5, 2009, deleted certain information from his Goldman desktop after the upload, and thereafter copied the information he had uploaded to the German server to three

different home computers and devices. (Compl. ¶ 13). The defendant claimed, however, that he only intended to collect "open source" code – *i.e.*, material not owned by Goldman – but that he uploaded more files than he intended. (*Id.*) Although not included in the Complaint, the Government expects to prove at trial that the defendant stated, in substance and in part, that he took steps to erase records of the transfer because he knew it was a violation of Goldman's policies.[2]

The next day, on July 4, 2009, the defendant was presented before a Magistrate Judge in the Southern District of New York and charged in Complaint 09 Mag. 1553 with theft of trade secrets and interstate transportation of stolen property. Bail conditions were set and the defendant was released on July 6, 2009, and has been on pretrial release since that date.

On February 11, 2010, a grand jury sitting in this district returned Indictment 10 Cr. 96 (DLC), which charges the defendant in three Counts: Count One charges the defendant with theft of trade secrets, in violation of Title 18, United States Code, Section 1832; Count Two charges the defendant with transportation of stolen property in interstate and foreign commerce, in violation of Title 18, United States Code, Section 2314; and

[2]If the Court wishes, the Government can provide a copy of a report summarizing the defendant's post-arrest statement, which has already been disclosed to the defendant in discovery, under separate cover.

Count Three charges the defendant with unauthorized computer access and with exceeding authorized access, in violation of Title 18, United States Code, Section 1030.

ARGUMENT

I. APPLICABLE LAW

A. Motion to Dismiss for Failure to State a Claim

The defendant seeks to dismiss all Counts of the Indictment for failure to state a claim because, he asserts, the facts alleged in the Indictment fail to establish violations of the offenses charged therein. The defendant's motion, made pursuant to Federal Rule of Criminal Procedure 12(b)(3)(B), is properly made "at any time while the case is pending." Fed. R. Crim. P. 12(b)(3)(B).

Federal Rule of Criminal Procedure 7(c) sets forth the minimal "notice" pleading standards required in federal criminal cases. Under Rule 7(c), an indictment must (i) contain a "plain, concise, and definite written statement of the essential facts constituting the offense charged" and (ii) "give the official or customary citation of the statute . . . that the defendant is alleged to have violated." Fed. R. Crim. P. 7(c). Rule 7(c) further provides that an Indictment may "allege that the means by which the defendant committed the offense are unknown or that the defendant committed it by one or more specified means." *Id*.

The Second Circuit has held that "'an indictment is sufficient if it, first, contains the elements of the offense charged and fairly informs a defendant of the charge against which he must defend, and, second, enables him to plead an

acquittal or conviction in bar of future prosecutions for the same offense.'" *United States v. Alfonso*, 143 F.3d 772, 776 (2d Cir. 1998) (quoting *Hamling v. United States*, 418 U.S. 87, 117 (1974)). In determining whether a count of an indictment sufficiently alleges an offense, each count of the indictment should be read "in its entirety." *United States v. Hernandez*, 980 F.2d 868, 871 (2d Cir. 1992). Moreover, "an indictment must be read to include facts which are necessarily implied by the specific allegations made." *United States v. Stavroulakis*, 952 F.2d 686, 693 (2d Cir. 1992) (internal quotation marks and citation omitted). In reading an indictment, "common sense and reason prevail over technicalities." *United States v. Sabbeth*, 262 F.3d 207, 218 (2d Cir. 2001).

An indictment does not have to set forth evidence explaining how the crime was committed or negating every defense. Because the indictment's purpose is to "fairly inform[] a defendant of the charge against which he must defend," *Alfonso*, 143 F.3d at 776 (quoting *Hamling*, 418 U.S. at 117), the Second Circuit has "repeatedly refused, in the absence of any showing of prejudice, to dismiss charges for lack of specificity." *United States v. Walsh*, 194 F.3d 37, 45 (2d Cir. 1999) (internal quotation marks and citation omitted). Indeed, the Second Circuit has consistently upheld indictments that "do little more than to track the language of the statute charged and state the time and

place (in approximate terms) of the alleged crime." *Alfonso*, 143 F.3d at 776 (internal quotation marks and citation omitted); *accord United States v. LaSpina*, 299 F.3d 165, 177 (2d Cir. 2002); *Walsh*, 194 F.3d at 44; *see also Hamling v. United States*, 418 U.S. 87, 117 (1974) ("It is generally sufficient that an indictment set forth the offense in the words of the statute itself.").

In this case, the defendant concedes that all Counts of the Indictment provide the defendant with sufficient notice of the charges against him, the elements of the offenses, and of how the defendant is alleged to have committed those offenses. (*See* Mem. 1 ("This is *not* a motion to dismiss the Indictment for failure to provide sufficient particulars to apprise the defendant of the charges against him. The Indictment is certainly specific enough to apprise Aleynikov of the essential elements of the three statutes the grand jury alleges he violated and to inform him and the Court of how the grand jury alleged he violated those statutes.") (emphasis in original)). Instead, the defendant argues that the factual allegations contained in the Indictment are insufficient to sustain the charges pending against him. (*See* Mem. 13 ("[N]one of the counts alleges facts that would under any circumstances bring Aleynikov's conduct within the meaning of the charged statutes.")) As the facts alleged in the Indictment fail to state a claim under the statutes charged, the

defendant argues, the Indictment is fatally defective and must be dismissed.

In the Second Circuit, courts may dismiss an indictment where the Government's proposed proof would not establish an offense as a matter of statutory interpretation. In *United States v. Mennuti*, 639 F.2d 107 (2d Cir. 1981), the Second Circuit affirmed a district court's dismissal of an indictment that charged a violation of the Organized Crime Control Act of 1970, Title 18, United States Code, Section § 844(i), because the Government's proposed proof did not satisfy the interstate commerce element of that statute as a matter of law. *Mennuti*, 639 F.2d at 108-109, 113. Likewise, in *United States v. Pacione*, 738 F.2d 567 (2d Cir. 1984), the Second Circuit affirmed a district court's decision to dismiss certain counts in an indictment where the district court had found that "the totality of facts asserted by the government to be provable against [the defendant] do not establish a violation of the statute." *Pacione*, 738 F.2d at 569.

In deciding motions to dismiss, such as the defendant's, where the defendant claims the factual allegations are insufficient to support the offenses charged in the Indictment, courts may look to the facts alleged in the Indictment and to any additional facts proffered by the Government. *United States v. Perez*, 575 F.3d 164, 166 (2d Cir. 2009) (holding that on a

pretrial motion to dismiss, it is not proper to weigh the sufficiency of the evidence underlying the indictment, "'[u]nless the government has made what can fairly be described as a full proffer of the evidence it intends to present at trial.'") (quoting *Alfonso*, 143 F.3d at 776-77); *see also*, *Mennuti*, 639 F.2d at 108 n.1 (accepting and reviewing a proffer of additional facts from the Government prior to dismissing the Indictment because it did not state an offense as a matter of statutory interpretation).[3]

B. Principles of Statutory Interpretation

Because the defendant's challenges to the Indictment involve matters of statutory interpretation, the Government reviews the principles of statutory interpretation below.

Generally, statutory construction "must begin with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose." *United States v. Albertini*, 472 U.S. 675, 680 (1985) (quoting *Park 'N Fly v. Dollar Park and Fly, Inc.*, 469 U.S. 189, 194 (1985)). Where the statute's language is "plain,

[3]It is unclear from the Second Circuit's opinion in *Pacione* whether the district court looked just to the facts alleged in the indictment or to any other evidence proffered by the Government before making its decision, although the latter is strongly suggested by the district court's statement that "the *totality of facts asserted by the government to be provable* against [the defendant] do not establish a violation of the statute." *Pacione*, 738 F.2d at 569 (emphasis added).

'the sole function of the courts is to enforce it according to its terms.'" *United States v. Ron Pair Enterprises, Inc.*, 489 U.S. 235, 241 (1989) (quoting *Caminetti v. United States*, 242 U.S. 470, 485 (1917)); *see also Connecticut National Bank v. Germain*, 503 U.S. 249, 253-54 (1992) ("We have stated time and again that courts must presume that a legislature says in a statute what it means and means in a statute what it says there.").

If this Court determines that the text of a statute is not clear, then the Court should "discern congressional intent by reading the text in light of the legal principles that operate in the relevant area of the law." *United States v. Figueroa*, 165 F.3d 111, 115 (2d Cir. 1998); *accord United States v. Bronx Reptiles, Inc.*, 217 F.3d 82, 86 (2d Cir. 2000) ("[T]he intent of Congress is our lodestar.").

II. COUNT ONE OF THE INDICTMENT STATES A CLAIM

The defendant argues that Count One of the Indictment must be dismissed because it fails to state a claim. Specifically, the defendant contends that none of the facts set forth in the Indictment satisfy the jurisdictional element of the theft of trade secrets offense charged in Count One, which requires that the allegedly stolen trade secret be related to a "product produced for or placed in interstate or foreign commerce." The defendant avers that Goldman's high-frequency trading system – the "product" in this case – is not a "product" that is "produced for or placed in interstate or foreign commerce" because Goldman does not license or sell it to others. The defendant's argument fails. The defendant adopts a construction of the interstate commerce requirement of the trade secrets statute that is not only not supported by the plain text of the statute and the statute's legislative history, but also appears at odds with the purpose of the trade secrets statute itself. As Goldman's high-frequency trading system has a strong and indisputable connection to both interstate and foreign commerce, there is no question that it is a "product produced for or placed in interstate or foreign commerce." Accordingly, the defendant's motion to dismiss Count One should be denied.

A. Relevant Facts

Count One of the Indictment charges the defendant with theft

of trade secrets, in violation of Title 18, United States Code, Section 1832. The statutory allegations from the Indictment for Count One read as follows:

> From at least in or about May 2009, up to and including on or about July 3, 2009, in the Southern District of New York and elsewhere, SERGEY ALEYNIKOV, the defendant, unlawfully, willfully, and knowingly, without authorization copied, duplicated, sketched, drew, photographed, downloaded, uploaded, altered, destroyed, photocopied, replicated, transmitted, delivered, sent, mailed, communicated, and conveyed a trade secret, as that term is defined in Title 18, United States Code, Section 1839(3), and attempted so to do, with intent to convert such trade secret, that was related to and included in a product that was produced for and placed in interstate and foreign commerce, to the economic benefit of someone other than the owner thereof, and intending and knowing that the offense would injure the owner of that trade secret, to wit, ALEYNIKOV, while in New York, New York and elsewhere, without authorization copied and transmitted to his home computer Goldman's proprietary computer source code for Goldman's high-frequency trading business, with the intent to use that source code for the economic benefit of himself and his new employer, Teza.
>
> (Title 18, United States Code, Sections 1832(a)(2), 1832(a)(4), & 2.)

(Ind. ¶ 16).

The charging language for Count One is preceded by nearly 10 pages of detailed factual allegations – which are also incorporated by reference into Count Two and Count Three – that are more than sufficient to make out a claim for theft of trade secrets. Among other things, the Indictment alleges that Goldman, which is headquartered in New York, New York and does business throughout the world, engages in "high-frequency trading

on various commodities and equities markets" (Ind. ¶ 1), which include national securities markets such as the NYSE and NASDAQ (*id*. ¶ 4), and that Goldman makes "many millions of dollars" in profits from its high-frequency trading. (*Id*. ¶ 5). The Indictment's factual allegations address both Goldman's trading algorithms, which are alleged to be "complex mathematical formulas" embodied in "computer programs" that "ma[k]e the trading decisions" (*id*. ¶¶ 4-5) and Goldman's "Platform," which is alleged to be a "system of computer programs" that "rapidly obtain[s] information related to the latest market movement and trends," "processe[s] that information into a form that could be analyzed by Goldman's trading algorithms," and then "execute[s] the [algorithms'] trading decisions." (*Id*. ¶¶ 4-5). The Indictment collectively refers to the algorithms and Platform as Goldman's "high-frequency trading," "high-frequency trading system," or "high-frequency trading business." (*See*, *e.g.*, *id.* ¶¶ 5, 7 ("Goldman's high-frequency trading system – the Platform and the trading algorithms – were comprised of different computer programs."), 16).

According to the Indictment, Goldman's high-frequency trading system, which "Goldman has not licensed . . . and has not otherwise made . . . available to the public" (Ind. ¶ 6), contains trade secrets which "confer[] a competitive advantage to Goldman with respect to its trades" (*id.* ¶ 5) and the

confidentiality thereof Goldman has "taken various measures to protect." (*Id.* ¶ 8).

The Indictment alleges that Goldman has hired "many" employees who have been responsible for "develop[ing] and maintain[ing] both the Platform and Goldman's trading algorithms." (Ind. ¶ 6). However, not all of Goldman's high-frequency trading system was developed internally by Goldman. The Indictment alleges that "Goldman acquired portions of the Platform, along with other assets, when it purchased the Hull Trading Company in or about 1999 for approximately $500 million." (*Id*.). The Government expects to prove at trial that the Hull Trading Company was headquartered in Chicago, Illinois.

Although not alleged in the Indictment, the Government expects to prove at trial that there are high-frequency trading systems (or components thereto) that may be purchased by companies seeking to engage in high-frequency trading.

The Government further expects to prove the following at trial. Goldman's high-frequency trading system trades on markets in the United States, Europe, and Asia. Goldman maintains computers in the United States and elsewhere in the world that conduct this trading activity.

B. Applicable Law

Title 18, United States Code, Section 1832 – the theft of trade secrets statute that is charged in Count One of the

Indictment – was enacted as part of the Economic Espionage Act of 1996 (the "EEA"). Section 1832 provides, in pertinent part:

> (a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly
>
> * * *
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
>
> * * *
>
> (4) attempts to commit any offense described in paragraphs (1) through (3) [is guilty of a crime].

18 U.S.C. § 1832(a)(2) & (4).

The EEA does not define the term "product" or the phrase "produced for or placed in interstate or foreign commerce" as used in Section 1832(a).

C. Discussion

The defendant argues that Count One should be dismissed because the Government cannot, on the facts alleged in the Indictment, satisfy the jurisdictional element of Section 1832. That element requires that the Government prove that the allegedly stolen trade secret be "related to or included in a product that is produced for or placed in interstate or foreign commerce." 18 U.S.C. § 1832(a). The defendant contends that the

"product" at issue here – Goldman's high-frequency trading system[4] – is simply not a "product that is produced for or placed in interstate or foreign commerce." Ignoring the obvious and indisputable connection between the Trading System – which executes scores of trades in securities and commodities markets in the United States and abroad – and interstate and foreign commerce, the defendant adopts an unduly narrow interpretation of the EEA that holds that the "product" refers only to tangible items that are sold to consumers through the stream of commerce. (Mem. 16-17). Because Goldman has never licensed or sold the Trading System, and does not presently have the intention of doing so, the defendant argues that the Trading System is therefore not a "product produced for or placed in" commerce within the meaning of the EEA and therefore Count One must be dismissed.[5]

---

[4]In his Memorandum of Law, the defendant characterizes Goldman's high-frequency trading system as the "Platform," (mem. 14-15 & n.3), despite the distinction made in the Indictment between the Platform and the trading algorithms. (*See* Ind. ¶¶ 4-6). Whatever term the defendant uses to describe Goldman's high-frequency trading system, the parties appear to agree that the relevant "product," for the purposes of this motion, is Goldman's entire trading system, which includes both the Platform (as defined in the Indictment) and the trading algorithms. The Government will hereinafter refer to Goldman's high-frequency trading system as the "Trading System."

[5]The Defendant argues that the Trading System is neither a "product" nor is it "produced for or placed in interstate or foreign commerce." The defendant analyzes each of these terms separately, devoting one section of his Memorandum of Law to arguing why the Trading System is not a "product" and another to

The defendant's argument fails. The defendant ignores the plain meaning of the EEA's jurisdictional element and instead looks to several other areas of the law – such as products liability – to import concepts that are simply inapplicable and inapposite in the context of the protection of trade secrets. A plain reading of the EEA reveals that the limitations proposed by the defendant are not warranted, and if the plain terms of the EEA are not clear enough, the legislative history and relevant legal context demonstrates that the EEA provides broad protection for trade secrets belonging to American companies. It is therefore clear that the Trading System – with its strong and indisputable connection to both interstate and foreign commerce – is a "product that was produced for or placed in interstate or foreign commerce."

The first step in statutory construction is to examine the plain meaning of the statute's terms. *See United States v. Albertini*, 472 U.S. 675, 680 (1985) (stating that statutory

---

arguing why the Trading System is not "produced for or placed interstate or foreign commerce." (Mem. 16, 25). Upon reviewing the defendant's arguments in each of these sections, however, it appears that they ultimately collapse into a single argument, as the defendant defines "product" and "produced for or placed in interstate or foreign commerce" nearly identically. (*Compare* Mem. 18 (defining "product" as something that "must be tangible personal property" that is "distributed commercially for use and consumption by the public") *with id*. 26 (defining "produced for or place in interstate or foreign commerce" as involving some "saleable, transportable good that was actually sold interstate or in foreign countries" or was developed for such distribution)).

construction "must begin with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose.") (quoting *Park 'N Fly v. Dollar Park and Fly, Inc.*, 469 U.S. 189, 194 (1985)). Here, Section 1832 requires that the "trade secret" in question must be "related to or included in a product that is produced for or placed in interstate or foreign commerce." 18 U.S.C. § 1832(a). The defendant does not dispute that the trade secrets that he allegedly stole are "related to or included in" the Trading System. Therefore, the only question for the Court is whether the Trading System is "a product that is produced for or placed in interstate or foreign commerce."

Applying the plain, ordinary meaning of the word "product," it is clear that the Trading System is a "product" within the meaning of the EEA. In this case, the Trading System is an integrated series of computer programs that work together to make fast, automated, and frequent trades in a variety of securities and commodities markets in the United States and abroad, generating many millions of dollars in profits. (Ind. ¶¶ 4-5). The Trading System was created by years of labor by developers at Goldman and from components that Goldman acquired from the Hull Trading Company. (*Id*. ¶ 6). The only difference between the Trading System and other computer software programs that would indisputably be a "product" under the defendant's narrow view –

such as Microsoft Windows – is that Goldman does not intend to sell or license the Trading System. Instead, Goldman uses it to conduct high-frequency trading in interstate and foreign commerce. This does not make the Trading System any less of a "product" and there is no reason for it not to be protected by the EEA.[6]

Likewise, it is clear that the Trading System is "produced for or placed in interstate or foreign commerce." The Trading System was created to trade securities and commodities in national and international markets; in other words, the Trading System's very reason for existence is to be engaged in interstate and foreign commerce. Accordingly, the Trading System clearly is something that was "produced for . . . interstate or foreign commerce," as anyone would understand the plain, common-sense meaning of those terms.

The Trading System is also something that is "placed in interstate or foreign commerce." The Trading System maintains both a physical presence and an electronic presence in the stream of commerce as it executes scores of orders to trade securities and commodities around the world. Thus, the Trading System has a

[6]Furthermore, although Goldman does not sell or license the Trading System, there are other high-frequency trading systems that are available for purchase. Accordingly, Goldman's trade secrets could also be said to relate to not just the Trading System, but to high-frequency trading systems generally, some of which are commercially available.

very real and tangible presence in the stream of commerce. This is certainly not a "secret trading system, internal to Goldman and destined to remain there, never to see the light of day" (Mem. 16), but a system that was produced for, and has a significant presence in, both interstate and foreign commerce. Thus, the Trading System is both "produced for or placed in interstate or foreign commerce."

The Government's view of the EEA is confirmed by the EEA's legislative history, which reveals that Congress intended to provide broad protection for trade secrets. According to the legislative history, the passage of the EEA was driven by two primary concerns. The first concern was that, as the value of intellectual property to the United States' economy increased, *see*, *e.g.*, H.R. Rep. 104-788, at 4, *reprinted in* 1996 U.S.C.C.A.N. 4021, 4023, 1996 WL 532685 (1996) (recognizing the growing importance of "proprietary economic information" and finding that "[a]s the nation moves into the high-technology, information age, the value of these intangible assets will only continue to grow."); *see also* S. Rep. 104-359, at 6, 1996 WL 497065 (1996) ("In the last few decades, intangible assets have become more and more important to the prosperity of companies."), so too were the number of attempts to steal that property. *See* H.R. Rep. 104-788, at 6, *reprinted in* 1996 U.S.C.C.A.N. at 4024 (citing a study that estimated "the potential losses for all

American industry [from economic espionage] could amount to $63 billion annually.").

Congress' second concern was that there was no comprehensive criminal law that protected proprietary information in a thorough and systematic manner. *See* S. Rep. 104-359, at 10 ("Developments in the law, however, have not kept pace with this rapidly changing environment."); H.R. Rep. 104-788, at 6-7, *reprinted in* 1996 U.S.C.C.A.N. at 4024-25 (noting the perceived limitations with existing state and federal laws). Accordingly, Congress promulgated the EEA to "extend vital federal protection to another form of proprietary economic information–trade secrets." H.R. Rep. 104-788, at 4, *reprinted in* 1996 U.S.C.C.A.N. at 4023.

In enacting the EEA, Congress addressed the threat of economic espionage from both foreign governments and others, such as insiders who steal their employer's trade secrets with the intent to benefit themselves or a new employer. *See* 142 Cong. Rec. H10460-01, at H10461, 1996 WL 525647 (1996) ("Generally speaking, these types of crime fall into two broad categories: First, there are thefts by foreign companies, often with the cooperation of foreign governments. . . . The second category of these crimes are committed by Americans or U.S. nationals who leave their employment and steal proprietary information which they deliver to new employers.").

The result was that the EEA contains two provisions

addressing trade secret theft. The first – 18 U.S.C. § 1831 – prohibits the theft of trade secrets by individuals with the knowledge and intent that the theft will benefit "any foreign government, foreign instrumentality, or foreign agent." 18 U.S.C. 1831(a). The second – 18 U.S.C. § 1832, which is charged in this case – prohibits the theft of trade secrets by individuals with the intent to benefit "anyone other than the owner thereof, and intending and knowing that the offense will[] injure the owner of that trade secret." 18 U.S.C. § 1832(a).

The defendant implies that the inclusion of the interstate commerce element in Section 1832 but not in Section 1831 reflects Congress' intent that Section 1832 should be applied to a narrower range of trade secrets than Section 1831. (*See* Mem. 23 n.5). However, the Government is not aware of anything in the legislative history that demonstrates that Congress intended Section 1832 to address a narrower set of trade secrets compared with Section 1831. In fact, the interstate commerce requirement is not mentioned when the two provisions are compared. For example:

> The crime of "economic espionage" [Section 1831] will require proof of intent or knowledge by the offender that the offense will benefit a foreign government, foreign instrumentality, or foreign agent through economic espionage. The crime of "theft of trade secrets" [Section 1832] will require proof of the offender's intention to convert a trade secret for the economic benefit of a person other than the owner and also the intent or knowledge by the offender that the offense will injure the owner of the trade secret.

142 Cong. Rec. H12137-01, at H12144, 1996 WL 553652 (1996). Thus, a more plausible explanation for the inclusion of the "product" requirement in Section 1832 but not Section 1831 is that Congress needed to supply a basis for federal jurisdiction to Section 1832, whereas Section 1831's jurisdictional nexus is supplied from its focus on the actions of foreign governments.

The general context of trade secrets law provides additional support for a broad reading of the EEA. Congress modeled the definition of "trade secret" in the EEA after the Uniform Trade Secrets Act, and intended that the definition to "be read broadly."[7] H.R. Rep. 104-788, 12, 1996 U.S.C.C.A.N. at 4031. The Uniform Trade Secrets Act provides for injunctive relief and damages for misappropriation of trade secrets, but does not require that the trade secrets be related to a specific commercial product. *See* Unif. Trade Secrets Act § 1 *et seq.* (amended 1985).

Likewise, the Restatement (Third) of Unfair Competition broadly defines "trade secret" as "any information that can be used in the operation of a business or other enterprise and that

---

[7]In fact, as noted by the Third Circuit in *United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998), "the EEA protects a wider variety of technological and intangible information than current civil laws," such as those based on the Uniform Trade Secrets Act. 155 F.3d at 196. "Trade secrets are no longer restricted to formulas, patterns, and compilations, but now include programs and codes, 'whether tangible or intangible, and whether or how stored.'" *Id*. (quoting Section 1839(3)).

is sufficiently valuable and secret to afford an actual or potential economic advantage over others." Restatement (Third) Unfair Competition § 39 (1995). The comments to this section make clear "trade secret" can relate any number of things, including "services":

> A trade secret can relate to technical matters such as the composition or design of a product, a method of manufacture, or the know-how necessary to perform a particular operation or service. A trade secret can also relate to other aspects of business operations such as pricing and marketing techniques or the identity and requirements of customers.

Id. cmt. d. Under the Restatement, "[a]n employee or former employee who uses or discloses a trade secret owned by the employer or former employer in breach of a duty of confidence is subject to liability for appropriation of the trade secret." *Id*. § 42.

Citing no cases actually interpreting the EEA in the manner that he proposes,[8] the defendant argues for a narrow

---

[8]The Government is not aware of any case addressing the scope of the interstate commerce requirement in Section 1832 in more than a cursory manner and none that address the specific issue raised by the defendant. For example, in one case, *United States v. Hsu*, 40 F. Supp. 2d 623 (E.D. Pa. 1999), the district court addressed the issue in just two sentences in a footnote, finding that a trade secret being developed for a future (and as yet nonexistent product) can relate back to an earlier (and existent) version of the "product" under development:

> In his motion papers and at oral argument . . . [the defendant] argued that the EEA does not apply to products or processes in research and development and, thus, the *Lopez* interstate or foreign commerce requirement – or indeed the statute's explicit

interpretation of the jurisdictional element, based primarily on the law of products liability, and relying on definitions of "product" provided in the Restatement (Third) of Torts: Products Liability and also on the definition of "product" from Black's Law Dictionary.[9] (Mem. 16-17). The defendant then relies on

---

> requirement for such commerce – was not met in this case. We rejected that argument because "second generation" taxol technology (the technology that defendant Hsu is accused of attempting and conspiring to steal, and which is not yet commercially viable) is clearly "related to," *see* EEA, 18 U.S.C. § 1832(a), the "first generation" taxol technology that Bristol-Myers Squibb currently uses to produce its Taxol from the bark of yew trees (*taxus brevifolia*).

40 F. Supp. 2d at 625 n.1. Similarly, in *United States v. Yang*, 281 F.3d 534 (6th Cir. 2002), the Sixth Circuit held that the evidence adduced at trial was sufficient to prove that a trade secret had a sufficient nexus to interstate commerce because it involved a product that generates millions of dollars of sales per year and is related to products sold in the United States and elsewhere. 281 F.3d at 551 & n.4. Rather than provide any support to the defendant's position, these cases stand merely for the uncontroversial proposition that the EEA requires that the trade secret at issue must "relate to" some product that has a connection to interstate and foreign commerce.

[9]The complete entry for "product" in Black's Law Dictionary cross-references the entries for "manufacturing" and "products liability," thus showing that Black's Law Dictionary has derived its definition of "product" from those specialized areas of law and business. If the Court were inclined to rely on a dictionary at all, the Government respectfully suggests that a better place to find the plain, common meaning of the word "product" would be an ordinary dictionary. *See Oxford English Dictionary Online* (June 2010 Draft Revision to 2d. ed. 1989) http://dictionary.oed.com/entrance.dtl (defining "product" as "[a]n object produced by a particular action or process; the result of mental or physical work or effort."); *American Heritage Dictionary College Dictionary* 1112 (4th ed. 2002) (defining "product" as "[s]omething produced by human or mechanical effort or by a natural process."); *Webster's Third New International*

cases interpreting the term "product" in the context of products liability and other inapposite areas of the law to advance his argument that "product," as used in the EEA, refers only to "a tangible item of personal property distributed to and used by the commercial public." (*Id*. 16-19).

The defendant's analogy fails because products liability law is addressed to issues that are different, and distinguishable, from those involved in intellectual property law. Unlike the law of intellectual property, the law of products liability is *necessarily* concerned with defective *goods* that cause physical or economic harm to the consumers who purchase them. *See*, *e.g.*, Restatement (Third) of Torts: Products Liability § 1 (1998) ("One engaged in the business of selling or otherwise distributing products who sells or distributes a defective product is subject to liability for harm to persons or property caused by the defect."). Quite naturally, then, "[p]roducts liability law is geared to the *tangible world*." Restatement (Third) Torts: Products Liability § 19 cmt.d (1998) (emphasis added).

By contrast, the law governing the protection of trade secrets is focused on the protection of intellectual property, which is often both *intangible* and valuable. *See* H.R. Rep. 107-788, at 4, *reprinted in* 1996 U.S.C.C.A.N. at 4023, 1996 WL 532685

Dictionary of the English Language 1810 (Philip Babcock Gove ed. 1993) (defining "product" as "something produced by physical labor or intellectual effort: the result of work or thought.").

("For many companies this information is the keystone to their economic competitiveness . . . As the nation moves into the high-technology, information age, the value of these intangible assets will only continue to grow."). The purpose of the EEA, according to its legislative history, is "to bring together into a single vehicle the prohibition on the theft of trade secrets and proprietary information by both private individuals and corporations and by foreign governments and those acting on their behalf." 142 Cong. Rec. S12201, at S12208, 1996 WL 559474 (1996); *see also Hsu*, 155 F.3d at 195 ("Congress recognized the importance of developing a systemic approach to the problem of economic espionage, . . . and stressed that only by adopting a national scheme to protect U.S. proprietary economic information can we hope to maintain our industrial and economic edge and thus safeguard our national security.") (quotations and citations omitted).

Accordingly, there is no reason – and the defendant provides none that are persuasive – why the EEA should be saddled with a definition of "product" that more properly addresses issues related to the manufacture and distribution of defective goods. As the legislative history cited above makes clear, the EEA is a forward-looking statute designed to protect confidential intellectual property in the "information age." The Second Circuit has stated that courts "have been instructed to 'free our

minds from the notion that criminal statutes must be construed by some artificial and conventional rule.'" *United States v. Bottone*, 365 F.2d 389, 394 (2d Cir. 1966) (quoting *United States v. Dege*, 364 U.S. 51, 52 (1960)); *see also United States v. Bramblett*, 348 U.S. 503, 509-10 (1955) ("That criminal statutes are to be construed strictly is a proposition which calls for the citation of no authority. But this does not mean that every criminal statute must be given the narrowest possible meaning in complete disregard of the purpose of the legislature."). Accordingly, it would be absurd if the EEA did not protect the Trading System, which, while not sold to consumers by the measure of products liability, is nonetheless a product that has an indisputable presence in interstate and foreign commerce.

The same holds true for the other areas of the law relied upon by the defendant to foist a narrow definition of "product" on the EEA. The Magnuson-Moss Warrant Act, relied upon by the defendant to argue that "product" in the EEA means "consumer product" (*see* Mem. 18), is concerned with the warranties for consumer products.[10] *See* 15 U.S.C. § 2301, *et seq.* It therefore is similar to the law of products liability in its focus on tangible goods sold to consumers and not persuasive as a means of interpreting EEA. Similarly, the Comprehensive Environmental

[10]Moreover, the term "consumer product" appears nowhere in the EEA.

Response, Compensation, and Liability Act, cited by the defendant in a case addressing the definition of "consumer product" (*see* Mem. 17), is even further removed from the realm of trade secrets, as it addresses environmental pollution. *See* 42 U.S.C. § 9601, *et seq.* Another case cited in the defendant's Memorandum of Law, *General Dynamics Corp. v. United States*, 202 Ct. Cl. 347, 1973 WL 21349 (1973), addressed whether and to what extent the developer of a prototype aircraft could be compensated by the Government under certain procurement regulations wholly inapposite to the instant case.[11]

With respect to the meaning of "produced for or placed in interstate or foreign commerce," the defendant relies on cases interpreting the Fair Labor Standards Act, 29 U.S.C. § 201, *et seq.* ("FLSA") (*see* Mem. 25-26), a statute which is directed at

---

[11]Specifically, in *General Dynamics*, the developer created a prototype aircraft and sought to obtain a contract to ultimately manufacture and sell such aircraft to the armed services. 1973 WL 21349, at *1-*5. After the aircraft crashed during a test flight, the Government and the developer became involved in a dispute over whether the design costs of the prototype aircraft, which had overrun the amount allotted to the developer in a contract with the Government, could be billed to the Government as "selling costs." *Id*. at *6. The Court of Claims quite naturally ruled that since no aircraft were actually sold, it was not appropriate to bill the Government for "selling costs." *Id.* at *6-*11. The defendant nonetheless relies on *General Dynamics* for the proposition that prototypes cannot be "products" because they are not intended for commercial sale, but are instead created to test design capabilities. (*See* Mem. 20). Thus, the defendant's position would have the absurd result of excluding from the protection of Section 1832 trade secrets that are related to prototypes.

labor standards in "industries engaged in commerce or in the production of goods for commerce." 29 U.S.C. § 202(a). The defendant relies on the FLSA cases cited in his Memorandum of Law for their interpretation of whether "goods" have been shipped in interstate and foreign commerce. (*See* Mem. 25-26). Unfortunately for the defendant, however, the word "goods" appears nowhere in the EEA, and therefore, these cases are unpersuasive here.[12]

The defendant next cites several trades secrets cases for the proposition that "the EEA reflects a focus on trade secrets relating to tangible products already sold, licensed or otherwise distributed." (Mem. 22-23). These cases, however, do not advance the defendant's argument. Certainly some, perhaps most, of the cases brought under Section 1832 will involve trade secrets that are related to products sold to customers in commerce. That does not lead to the conclusion, however, that the Trading System is outside the scope of Section 1832. In fact, the Government is aware of other cases under Section 1832 in which the trade secret does not appear to be related to a

[12]Ironically, certain terms defined in the FLSA are consistent with the Government's broad reading of the EEA's requirement that the "product" be "produced for or placed in" commerce. For example, the FLSA defines "commerce" as "*trade*, *commerce*, transportation, *transmission*, or *communication* among the several States or between any State and any place outside thereof," and "produced" as "produced, manufactured, mined, handled, or *in any other manner worked on* in any State." 29 U.S.C. § 203(b) & (j) (emphasis added).

"product" that fits within the defendant's circumscribed definition. For example, in *United States v. Nosal*, No. CR 08-00237 MHP, 2009 WL 981336 (N.D. Cal. Apr. 13, 2009), the stolen trade secrets were names and contact information from a database maintained by an executive search firm, which the defendants – former employees of the firm – allegedly stole with the intent to use in a competing venture. 2009 WL 981336, at *1.

Finally, the defendant relies on Department of Justice practice manuals and law journal articles to bolster his argument that "an item constitutes a 'product' under the EEA only if it is developed or actually distributed for public use and consumption." (Mem. 21-22, 24). The three journal articles the defendant cites provide only cursory (and substantially similar) analysis of the interstate commerce requirement with no citation to authority other than to Section 1832 itself. (*See* Mem. 24). Even so, a fair reading of these articles show that their discussion of the relevant language in Section 1832 – "product produced for or placed in interstate or foreign commerce" – is directed at distinguishing between trade secrets related to products and trade secrets related to pure services, or trade secrets that are not used by a company in any fashion. For example:

> Because trade secrets explicitly must be embodied in a product in the stream of commerce, protection is limited if the trade secret related to a *rendering of services* rather than a produced ware that contains or uses the secret. As

> noted by some commentators, "[t]his means that the EEA arguably does not cover *either 'negative know-how' or information discovered but not [currently] used by a company*.

Spencer Simon, *The Economic Espionage Act of 1996*, 13 Berkeley Tech. L.J. 305, 315 (1998) (emphasis added). The Trading System is neither a "service" nor is it "negative know-how" that is not used by Goldman. To the extent that these article are in accordance with the defendant's narrow interpretation of the EEA, they are unpersuasive for the reasons stated above.

The defendant's references to the United States Attorneys' Manual ("USAM") or the Department of Justice's Intellectual Property Crimes manual ("IP Manual") are similarly unpersuasive.[13] The IP Manual provides, among other things, that "[t]o prove that the product was produced for interstate or foreign commerce, the government need only show the victim's intent to distribute the product or *utilize the process under development for a product*," and "[a]lthough the 'product'

---

[13]The guidance expressed in those manuals is not binding on the Government in this case. *See* USAM 1-1.100 ("The Manual provides only internal Department of Justice guidance. It is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal. Nor are any limitations hereby placed on otherwise lawful litigative prerogatives of the Department of Justice.") and IP Manual, initial page ("The contents of this book provide internal suggestions to Department of Justice attorneys. Nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter by any prospective or actual witnesses or parties. *See United States v. Caceres*, 440 U.S. 741 (1979).")

requirement is not discussed in the legislative history, the term's plain meaning appears to *exclude pure services such as technical skills and know-how* that are not embodied in or related to a saleable, transportable good." IP Manual at 160-61 (emphasis added). Likewise, the section of the USAM cited by the defendant states:

> In cases where the trade secret is related to a product actually being manufactured and sold, this element is easily established by evidence of interstate sales. Where the trade secret relates to a product in research and development, proof might be more difficult. *However, there is no evidence that Congress intended to create such a large exception to the trade secrets accorded protection under the EEA*. Therefore, in cases in which the trade secret is related to a product still being developed but that product will ultimately be sold in interstate commerce, prosecutors should establish this fact, and argue that it sufficiently meets this element.

USAM 9-59.100 (emphasis added). What these passages teach is that in the typical case under Section 1832, it will be fairly easy to prove the interstate commerce requirement by introducing evidence of sales of a product to which the stolen trade secret is related, or if there are no current sales, evidence that the trade secret is related to product that is under development. The IP Manual further states that Section 1832 does not apply to pure services, "such as such as technical skills and know-how," a description that clearly does not apply to the Trading System. IP Manual at 161. What is clear from these practice manuals is that the Trading System was not in the minds of their authors

when the manuals were written, and that their guidance, to the extent it even supports the defendant's position,[14] is directed at the generic trade secrets case, but not this one.

Accordingly, the defendant's motion to dismiss Count One of the Indictment should be denied.

III. COUNT TWO OF THE INDICTMENT STATES A CLAIM

The defendant argues that Count Two of the Indictment – which charges the defendant with interstate and foreign transportation of stolen property in violation of Title 18, United States Code, Section 2314 – fails to state a claim because the "proprietary computer source code for Goldman's high-frequency trading business" that the defendant allegedly stole does not constitute "goods, wares, merchandise, securities or money" as a matter of statutory interpretation, and therefore must be dismissed. Again, the defendant's argument fails, as the material stolen by the defendant is, by any fair reading of Section 2314, "goods, wares, or merchandise."

A. Relevant Facts

Count Two of the Indictment charges the defendant with transportation of stolen property in interstate and foreign commerce, in violation of Title 18, United States Code, Section

[14]For example, the IP Manual emphasizes that "[t]he nexus to interstate or foreign commerce [in Section 1832] appears to have been intended *merely* to allow federal jurisdiction." IP Manual at 160 (emphasis added).

2314.[15] The statutory allegations from the Indictment for Count Two read as follows:

> From in or about June 2009, up to and including in or about July 2009, in the Southern District of New York and elsewhere, SERGEY ALEYNIKOV, the defendant, unlawfully, willfully, and knowingly, transported, transmitted, and transferred in interstate and foreign commerce goods, wares, merchandise, securities, and money, of the value of $5,000 and more, knowing the same to have been stolen, converted and taken by fraud, to wit, ALEYNIKOV, while in New York, New York, copied, without authorization, Goldman's proprietary computer source code for Goldman's high-frequency trading business, the value of which exceeded $5,000, uploaded the code to a computer server in Germany, and carried that stolen code to a meeting with his new employer, Teza, in Chicago, Illinois.
>
> (Title 18, United States Code, Sections 2314 & 2.)

(Ind. ¶ 18).

Count Two alleges that the defendant transported the stolen source code across state and foreign boundaries on two occasions; first, when the defendant uploaded the stolen source code from Goldman's computer system to the computer server in Germany and second, when the defendant carried the stolen source code with him to a meeting at his new employer in Chicago, Illinois. (Ind.

---

[15]Title 18, United States Code, Section 2314 provides, in pertinent part:

> Whoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud [commits a crime].

18 U.S.C. § 2314.

¶ 18). As with the other counts of the Indictment, Count Two is supported by 10 pages of detailed factual allegations.

The Indictment alleges that the stolen source code related to Goldman's high-frequency trading system. (Ind. ¶ 7). Goldman's high-frequency trading system, the "Trading System," as defined above, was composed of computer programs that contained trading algorithms and programs related to the Platform. (Ind. ¶ 7). The Indictment defines "source code" as "a series of programming instructions, in a human-readable format, that specify the actions to be performed by a computer program." (*Id*.) The source code allegedly stolen by the defendant related to computer programs that were part of the Trading System. (*Id*. ¶ 12).

The Indictment alleges that at the very end of the defendant's last day at Goldman's offices – June 5, 2009 – the defendant, without authorization, executed a number of commands and programs at his Goldman work computer that resulted in hundreds of thousands of lines of the Trading System's source code being copied, compressed, encrypted, and finally uploaded from Goldman's computer network to a storage server located in Germany. (Ind. ¶ 12). Later that day, while at home, the defendant downloaded the stolen source code to his home computer, and thereafter copied it to some of his other computers and electronic devices. (*Id*. ¶ 13). The Indictment further alleges

that the defendant stole source code through a variety of means throughout his employment at Goldman, and had saved that stolen source code on various of his computer computers and electronic devices. (*Id.* ¶ 14). On July 2, 2009, the defendant traveled to Chicago, Illinois for meetings at Teza's offices, carrying with him a laptop computer and a flash drive, each of which contained source code for the Trading System, including some of the source code the defendant uploaded on June 5, 2009. (*Id*. ¶ 15).

Goldman acquired some of the components of the trading system when it purchased the Hull Trading Company. (Ind. ¶ 6). Although not alleged in the Indictment, the Government expects to prove at trial that there are high-frequency trading systems (and components thereto) that may be purchased or licensed by entities seeking to engage in high-frequency trading. The Government also expects to prove at trial that the source code stolen by the defendant has value to any company that is seeking to start a high-frequency trading business.

B. Discussion

The defendant contends that Count Two must be dismissed because the allegedly stolen source code is not "goods, wares, merchandise, securities or money" as required to state a claim under Section 2314. (Mem. 27-35). The defendant avers that Section 2314 was originally enacted at a time when Congress was more concerned with stolen automobiles than with stolen computer

code and is therefore not suited for prosecutions such as the instant case. The defendant relies on a number of cases to assert that Section 2314 applies only to tangible goods, wares, and merchandise, and not to "intangible" property like source code.

The defendant's argument is unpersuasive. Contrary to the defendant's assertions, the stolen source code falls squarely within the scope of Section 2314 and the defendant's assertion that the stolen property must be "tangible" is incorrect. A fair reading of the cases cited by the defendant and the law of this Circuit demonstrates that even "intangible" property – such as confidential business information – may be covered by Section 2314 if the property is ordinarily the subject of commerce. Further, the defendant's contention that Section 2314 excludes all intellectual property from its purview is based on a misreading of the Supreme Court's decision in *Dowling v. United States*, 473 U.S. 207 (1985). To the extent that courts in other circuits have expanded *Dowling*'s holding, those decisions are not binding here, are not persuasive, and are not consistent with the Second Circuit's decisions.

Section 2314 does not define the terms "goods, wares, merchandise, securities or money." The Second Circuit, however, has addressed the meaning of those terms in two cases that are relevant here. In *United States v. Bottone*, 365 F.2d 389 (2d

Cir. 1966), the defendants were convicted under Section 2314 of stealing the laboratory cultures and papers outlining the confidential manufacturing processes of a drug manufacturer. On appeal, one of the defendants challenged whether the stolen papers were "goods, wares, merchandise, securities or money" under Section 2314. *Bottone*, 365 F.2d at 393. Citing the Third Circuit's decision in *United States v. Seagraves*, 265 F.2d 876, 880 (3d Cir. 1959), the Second Circuit stated that there is "not any doubt on our part that papers describing manufacturing procedures are goods, wares, or merchandise" under Section 2314. *Bottone*, 365 F.2d at 393 (citing *United States v. Seagraves*, 265 F.2d 876, 880 (3d Cir. 1959) (holding that "[t]he terms 'goods, wares, merchandise" is a general and comprehensive designation of such personal property or chattels as are ordinarily a subject of commerce")). In *Bottone*, the Court of Appeals was persuaded that there was a market – albeit an illegal black market – for both the stolen laboratory cultures and stolen papers: "[t]he combination of [the value of the processes that were stolen] with the lack of patent protection in certain foreign countries created a market for stolen cultures and secret processes." *Id*. at 391.

The Second Circuit also addressed whether "papers" are "goods, wares, or merchandise" under Section 2314 in *In re Vericker*, 446 F.2d 244 (2d Cir. 1971). In *Vericker*, the Court of

Appeals considered whether a federal grand jury could properly investigate, as a violation of Section 2314, the theft of confidential law enforcement documents. 446 F.2d at 248. The Court of Appeals noted that the legislative history of Section 2314 "expressed an intention to cover all property," and found that "[i]t is quite true that under some circumstances mere papers may constitute goods, wares, or merchandise" within the meaning of the statue. *Id.* (quotations omitted). The Court stated, however, that such "papers" would be "within the normal meaning of goods, wares, or merchandise" only if they "'are ordinarily a subject of commerce.'" *Id*. (quoting *United States v. Seagraves*, 265 F.2d at 880). The Court then held that the stolen law enforcement documents – which concerned a criminal investigation being conducted by the FBI – were not "goods, wares, or merchandise" within the meaning of Section 2314 because they were not "ordinarily bought or sold in commerce, and the Government has not come forward or proffered any evidence to that effect." *Id*.

Thus, *Vericker* and *Bottone* teach that the test for determining whether confidential information – such as the trade secrets in *Bottone* – is a "good[], ware, or merchandise" is based upon whether the property is "ordinarily a subject of commerce." *Vericker*, 446 F.2d at 248; *see also United States v. Caparros*, No. 85 Cr. 990 (JFK), 1987 WL 8653, at *4 (S.D.N.Y. Mar. 25,

1987) ("When read together, *Bottone* and *In re Vericker* stand for the proposition that documents are covered by § 2314 provided there is a market for the material, be it either a legitimate market, or a black market.").

District courts applying *Bottone* and *Vericker* have found that Section 2314 applies to a variety of confidential business information. *See Caparros*, 1987 WL 8653, at *4 (finding secret business plans may be "goods, wears or merchandise" under Section 2314 if a market for those plans exists); *United States v. Farraj*, 142 F. Supp. 2d 484, 487-88 (S.D.N.Y. 2001) ("The Trial Plan at issue here, however, as is true for trial plans generally, was the work product of a business relationship between client and attorney, and may thus be viewed as an ordinary subject of commerce, created for a commercial purpose and carrying inherent commercial value at least as to the persons directly interested in the matter."); *United States v. Riggs*, 739 F. Supp. 414, 420 (E.D. Ill. 1990) (finding confidential information related to emergency 911 services provided by business to be "goods, wares, or merchandise" within the meaning of Section 2314); *but see United States v. Kwan*, No. 02 Cr. 241 (DAB), 2003 WL 22973515, at *6 (S.D.N.Y. Dec. 17, 2003) (finding that a travel agency's proprietary lodging and transportation contact lists and rate sheets were not "goods, wares, or merchandise" because at trial the Government adduced no evidence

that established the existence of a market, "legal or otherwise," for the confidential corporate documents).

Thus, there can be no question that confidential business information – whether it is secret business plans, information regarding the manufacture of a medicine, information regarding an attorney's trial plan, *or the source code to a high-frequency trading system* – can be "goods, wares, or merchandise" under Section 2314 if the information is ordinarily the subject of commerce.

In this case, the source code stolen by the defendant is clearly the "subject of commerce." The Government reviewed, in great detail above, how the Trading System is directly engaged in commerce around the world. Moreover, the Government expects to prove at trial that there is a market for high-frequency trading systems and that, in fact, Goldman acquired part of its trading system when it purchased the Hull Trading Company in 1999. Furthermore, the Government expects to prove that the stolen source code has value to any company that is seeking to start a high-frequency trading business.

That the stolen source code is "intangible" – in that it was transferred electronically from Goldman's computers to a server in Germany or that it is saved the defendant's laptop computer and flash drive – is immaterial. "The text of § 2314 makes no distinction between tangible and intangible property, or between

electronic and other manner of transfer across state lines." *Farraj*, 142 F. Supp. 2d at 488. In fact, in 1988, Section 2314 was amended to add the verbs "transmits" and "transfers" to make it clear that the statute "is not limited to the physical transportation of stolen or fraudulently acquired money or *property* but also extends to the situation in which such proceeds are transmitted or transferred electronically in interstate or foreign commerce." *United States v. Piervinanzi*, 23 F.3d 670, 678 n.6 (2d Cir. 1994) (emphasis added). Even prior to this amendment, the Second Circuit recognized, in the context of stolen money, that Section 2314 may be applied to electronic transfers:

> The manner in which funds were moved does not affect the ability to obtain tangible paper dollars or a bank check from the receiving account. Indeed, we suspect that actual dollars rarely move between banks, particularly in international transactions . . . The primary element of this offense, transportation, "does not require proof that any specific means of transporting were used."

United States v. Gilboe, 684 F.2d 235, 238 (2d Cir. 1982) (quoting *Pereira v. United States*, 347 U.S. 1, 9 (1954)). In *Bottone*, the Second Circuit held that "when the physical form of the stolen goods is secondary in every respect to the matter recorded in them, the transformation of the information in the stolen papers into a tangible object never possessed by the original owner should be deemed immaterial." *Bottone*, 365 F.2d at 393-94. Finally, the district court in *Riggs* explained that

it should therefore make no difference whether the information is printed on a paper or emailed across state lines:

> Therefore, in the instant case, if the information in Bell South's E911 text file had been affixed to a floppy disk, or printed out on a computer printer, then [the defendant's] transfer of that information across state lines would clearly constitute the transfer of "goods, wares, or merchandise" within the meaning of § 2314. This court sees no reason to hold differently simply because [the defendant] stored the information inside computers instead of printing it out on paper. In either case, the information is in a transferrable, accessible, even salable form.

739 F. Supp. at 421.

The defendant relies on *Dowling v. United States*, 473 U.S. 207 (1985), to argue that Section 2314 applies only to tangible objects. (Mem. 29-3). The holding in *Dowling*, however, is distinguishable from the circumstances present in the instant case. As the Judge Victor Marrero in *Farraj* noted:

> In *Dowling,* the Supreme Court held that where the victim holds only a copyright, distinct from the possessory interest of the owner of a simple good, and the only act charged involves an unauthorized infringement of that copyright, there is no violation of § 2314.

Farraj, 142 F. Supp. 2d at 489.[16] The defendant also relies on

[16]The Court's decision in *Dowling* appears to be motivated almost entirely by the special circumstances presented by copyright law, none of which are present here. The *Dowling* Court held that "Congress had no intention to reach copyright infringement when it enacted § 2314." *Dowling*, 473 U.S. at 226. The Court reached this conclusion after carefully analyzing the Constitutional and statutory bases for copyright law, the particular rights provided to copyright holders, and the types of copyright infringement that Congress has determined merits criminal sanction. *Id*. at 216-226. The Supreme Court stated

United States v. Brown, 925 F.2d 1301 (10th Cir. 1991), which held that "purely intellectual property" is not "goods, wares or merchandise" within the meaning of Section 2314. *Brown*, 925 F.2d at 1307. However, "the reasoning in *Brown* . . . may be based on a misapplication of *Dowling*."[17] *Farraj*, 142 F. Supp. 2d at 489. Therefore, *Brown*'s holding is not persuasive here.

The defendant also relies on *United States v. Stafford*, 136 F.3d 1109 (7th Cir. 1998). *Strafford*, however, is distinguishable on its facts and not sufficiently detailed to provide guidance. The "property" at issue in *Stafford* was "Comdata codes," which were transmitted to truck drivers to allow

---

that copyright is "no ordinary chattel," because it "comprises a series of carefully defined and carefully delimited interests to which the law affords corresponding exact protections," and therefore "does not easily equate with theft, conversion, or fraud." *Id*. at 216-17.

[17]In fact, while the Supreme Court in *Dowling* makes reference to "kindred fields of intellectual property law," such as patents and trademarks, *see Dowling*, 473 U.S. at 226, it does not make reference to trade secrets or confidential business information. The exclusion of trade secrets from the analysis in *Dowling* makes sense, as the reasons offered by the Supreme Court for excluding copyrighted works from the scope of Section 2314 do not apply to trade secrets. For example, whereas the Supreme Court notes that misappropriation of copyrighted materials is not even called "theft" under copyright law, *see id*. at 217, the misappropriation of trade secrets is called theft under trade secrets law. And whereas copyright holders are compelled to license their works under certain conditions, and are compelled to allow others the "fair use" of their copyrighted material, *see id*., no such conditions are imposed on the holders of trade secrets. Accordingly, there is no reason to believe that the Supreme Court intended to place all forms of intellectual property out of the reach of Section 2314.

the drivers to obtain cash at tellers at truck stops. *Stafford*, 136 F.3d at 1111. The Seventh Circuit held that these codes were "simply sequences of digits," which "have no value in themselves" but are merely "information," and therefore not "goods, wares or merchandise." *Id*. at 1114-15. By contrast, the source code in this case has a value in and of itself. In addition, because the charges in *Strafford* do not reveal how the defendant actually transported the codes across interstate boundaries, *id*., *Strafford* can only provide limited guidance here.

The defendant relies on a passage in *Bottone* where the Second Circuit states that "where no tangible objects were ever taken or transported, a court would be hard pressed to conclude that 'goods' had been stolen and transported within the meaning of § 2314." (Mem. 30). The defendant ignores, however, what is written immediately afterward, which indicates that what the *Bottone* Court had in mind was a "case where a carefully guarded secret formula was memorized, carried away in the recesses of a thievish mind and placed in writing only after a boundary had been crossed." *Bottone*, 365 F.2d at 393. This is not the case here, as the defendant did not memorize the source, but instead caused it to be transferred across interstate and foreign boundaries.

In sum, it is clear from a review of these authorities that (i) confidential business information is "goods, wares, and

merchandise" under Section 2314 when there is a market for that information and (ii) it is immaterial whether the information is stolen and transported in tangible or electronic form. Indeed, it would be odd if it was a violation of Section 2314 when confidential business information written on a piece of paper is stolen and physically transported across state lines, but not when that same information is transmitted electronically through an interstate or international wire. Accordingly, the defendant's motion with respect to Count Two of the Indictment should be denied.

IV. COUNT THREE OF THE INDICTMENT STATES A CLAIM

The defendant argues that Count Three – which charges the defendant with unauthorized computer access and exceeding authorized access in violation of the Computer Fraud and Abuse Act ("CFAA") – must be dismissed because it fails to state a claim. Relying on cases that have adopted an unduly constricted view of liability under Section 1030, the defendant contends that because he was authorized by Goldman to access the Trading System's source code to perform his duties as a Goldman employee, there can be no criminal liability under Section 1030 if he transferred the source code to his home computers in clear violation of Goldman's confidentiality policies and security protocols, and with the intent to convert the source code to his own use. This argument fails. Although the defendant is correct

in noting that courts are divided on the scope of liability under Section 1030, the view more consistent with a common sense and a plain reading of the statute would find that the defendant was not authorized to steal the source code from Goldman's system and that he exceeded whatever authorization he had when he did so.

A. Relevant Facts

Count Three of the Indictment charges the defendant with unauthorized computer access and exceeding authorized computer access, in violation of Title 18, United States Code, Section 1030(a)(2)(C). The statutory allegations of Count Three read as follows:

> In or about June 2009, in the Southern District of New York and elsewhere, SERGEY ALEYNIKOV, the defendant, unlawfully, intentionally, and knowingly, and, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States and of any State, accessed a protected computer without authorization and exceeded authorized access, which computer was used in and affecting interstate and foreign commerce and communication, and thereby obtained information from such protected computer the value of which exceeded $5,000, to wit, ALEYNIKOV, while in New York, New York, in violation of Goldman's policies and his confidentiality agreement with Goldman, accessed a computer server maintained by Goldman and copied Goldman's proprietary computer source code for Goldman's high-frequency trading business, the value of which exceeded $5,000, uploaded the code to a computer server in Germany, and then downloaded it to his home computer, all with the intent to use that source code for the economic benefit of himself and his new employer, Teza.
>
> (Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i)-(iii) and 2.)

(Ind. ¶ 20).

As alleged in the Indictment, Goldman limited access to the Trading System's source code to those employees "who had reason" to access it, such as the defendant, who was "a member of a team of computer programmers responsible for developing and improving certain aspects of the Platform." (Ind. ¶¶ 8(b), 9). As part of its security measures, Goldman "block[ed] certain transfers of information outside of Goldman's computer network and monitor[ed] some transfers of information by employees outside of Goldman's computer network." (*Id*. ¶ 8(c)).

Goldman required all of its employees to agree to a confidentiality agreement that provided that employees where to hold in "strict confidence" all "non-public information and materials," such as "information and materials describing or relating to the business and financial affairs," "operating procedures," and "policies and procedures of Goldman." (Ind. ¶ 8(d)). Employees also agreed to "irrevocably assign to Goldman" all work and inventions developed in the course of employment. (*Id*.). While employed by Goldman, the defendant was responsible for working on the Platform, but "[a]t no time during his employment" was the defendant "responsible for developing or maintaining any of Goldman's trading algorithms." (*Id*. ¶ 9).

As alleged in the Complaint, Goldman employees who had access Trading System's code were "instructed that they are not

permitted, without prior authorization, to distribute or transmit that code outside of [Goldman's] computer network." (Compl. ¶ 4(b)). The confidentiality agreement with Goldman further provided that at the termination of his employment with Goldman, the defendant was to return to Goldman any of Goldman's non-public information that the defendant had in his possession. (*Id.*).

The Indictment alleges that at 5:20 p.m. on June 5, 2009, the defendant's last day in Goldman's offices, the defendant undertook a series of steps to upload some of the Trading System's source code to a website in Germany that was outside of Goldman's computer system. (Ind. ¶ 12). The defendant thereafter downloaded the source code from that website to his home computers. (*Id.*). The Indictment alleges that the defendant uploaded the source to the German server "to evade various security blocks and monitoring features" designed to protect Goldman's "proprietary systems from theft." (*Id.*). After completing the upload, the defendant deleted certain information from his Goldman computer "to hide the fact that he copied, encrypted, and transferred proprietary Goldman files." (*Id.*) The defendant's upload of the Trading System's source code files to the German server was "without authorization from Goldman and in violation of Goldman's policies." (*Id.* ¶ 12(b)).

While not alleged in the Indictment, the Government expects

to prove that after the defendant's arrest he stated the following, in substance and in part: (i) the reason the defendant deleted his bash history and the encryption program on June 5, 2009 was because Goldman's policy would not allow him to transfer files out of Goldman's system and (ii) the defendant uploaded the source code to the particular website in Germany because it was a source code storage website that was not blocked by Goldman's security permissions.[18]

B. Relevant Law

Title 18, United States Code, Section 1030(a)(2)(C), provides, in pertinent part

> Whoever–
>
> * * *
>
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--
>
> * * *
>
> (C) information from any protected computer [is guilty of a crime].

18 U.S.C. § 1030(a)(2)(C).

The statute does not define "authorized access." The statute does define "exceeds authorized access" as "to access a

[18]As the Government noted above, these statements are taken from a report of the defendant's post-arrest statement that has already been disclosed to the defendant. If the Court wishes to see the complete report, the Government will provide it under separate cover.

computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

C. Discussion

The defendant correctly notes that courts are divided in interpreting the scope of criminal liability under Section 1030, specifically as to whether a potential defendant's access to a computer system was authorized or whether it "exceeds authorized access." (Mem. 36-37). Some courts, relied upon by the defendant, have taken an unduly narrow view of liability under Section 1030. They hold, essentially, that when examining whether access is unauthorized or exceeding authorization, a court must look only to whether a defendant had authorization to access the information in question, and not at the defendant's intentions in accessing the information or whether the defendant's access violated any employment or confidentiality agreements, or any duties owed to, the information's owner. *See, e.g.*, *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009) ("No language in [the CFAA] supports LVRC's argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest. Rather, the definition of 'exceeds authorized access' in § 1030(e)(6) indicates that Congress did not intend to include such an implicit limitation in the word 'authorization.'"); *Shamrock*

Foods Co. v. Gast, 535 F. Supp. 2d 962, 968 (D. Ariz. 2008) ("Here, Gast was authorized to initially access the computer he used at Shamrock. Further, Shamrock conceded that Gast was permitted to view the specific files he allegedly emailed to himself. Gast did not access the information at issue 'without authorization' or in a manner that 'exceed[ed] authorized access."); *Black & Decker Inc. v. Smith*, 568 F. Supp. 2d 929, 934 (W.D. Tenn. 2008) ("[T]he CFAA targets the unauthorized procurement or alteration of information, not its misuse."); *Diamond Power Int'l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007) (holding that "a violation does not depend upon the defendant's unauthorized use of *information*, but rather upon the defendant's unauthorized use of *access*."); *Int'l Assoc. of Machinists and Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479, (D. Md. 2005) (holding that complaint failed to state a claim under Section 1030 because the defendant, an officer in a union, was authorized to access the confidential information she accessed and misused).

A recent case, *Orbit One Communications, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373 (S.D.N.Y. 2010), is typical of the cases the defendant relies upon. In that case, Judge Lewis A Kaplan held that Section 1030 "supports a narrow reading," and that the statute "expressly prohibits improper 'access' of computer information," but does "not prohibit misuse or

misappropriation." *Orbit*, 692 F. Supp. 2d at 385. In *Orbit*, the district court set out several reasons for its holding. First, it looks to the terms "access without authorization" and "exceeds authorized access" as used in the statute, finding that an interpretation of those terms that encompasses an employee's misuse "would depart from the plain meaning of the statute." *Id*. Next, the district court looked to Section 1030's damages provisions and found that they appear to be focused on unauthorized intrusions by outsiders seeking to "compromis[e] the integrity and availability of data and may cause an interruption of computer service," and not on "competitive harm suffered as a result of misuse or misappropriation." *Id*. at 385-86. Finally, the district court was persuaded by the rule of lenity that a narrow reading of Section 1030 should be adopted so as not to "transform the common law civil tort of misappropriation of confidential information into a criminal offense." *Id*. at 386 (citations omitted).

By contrast, another line of cases takes a broader view of Section 1030, finding that individuals who initially had authorization to access information may exceed that authorization or be without authorization depending on the purpose for which they access the information, and whether their actions involve the violation of any confidentiality agreements or policies, or other obligations to the information's owner. *See*, *e.g.*, *United*

States v. Morris, 928 F.2d 504, 510 (2d Cir. 1991) (holding, in a case where a student who used his access to a university's computer system to upload malicious software which spread throughout the internet, that the defendant "did not use [the services to which he had authorized access] in any way related to their intended function. He did not send or read [e-mail] nor discover information about other users; instead, he found holes in both programs that permitted him a special and unauthorized access route into other computers."); *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006) (holding that employee's authorization to access computer terminated when the employee destroyed files "in violation of the duty of loyalty that agency law imposes on an employee"); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582-83 (1st Cir. 2001) (finding that former employees of EF who left to work for startup rival Explorica "exceeded authorized access" when they used proprietary information obtained from EF to glean information about EF's prices from its public website in violation of the "broad confidentiality agreement" that the employees had signed with EF.); *Calyon v. Mizuho Securities USA, Inc.*, No. 07 Civ. 2241 (RO), 2007 WL 2618658 (S.D.N.Y. Sept. 5, 2007) ("[T]he plain language of the statute seems to contemplate that, whatever else, 'without access' and 'exceeds authorized access' would include an employee who is accessing documents on a computer system which

that employee had to know was in contravention of the wishes and interests of his employer."); *Shurgard Storage Ctrs, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (holding that plaintiff stated a claim under 18 U.S.C. § 1030(a)(2) because employee-defendants "lost their authorization . . . when they allegedly obtained and sent proprietary information to [a rival company] via e-mail.").

For example, in *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000), Judge Barbara S. Jones addressed whether Section 1030(a)(2)(C) is violated if an entity uses information obtained from a public website in a way that violates the website's terms of service. Register.com is a domain-name registrar for the internet and provides a WHOIS database that provides contact information for customers who register for domain names through the registrar. *Register.com*, 126 F. Supp. 2d at 241-42. Register.com allows the public to access its WHOIS database, but requires that anyone wishing to search the database assent to terms of service which prohibited the use of automated programs to mine the database for information. *See id*. at 242-43. The terms of service also prohibited the use of information from the database for unsolicited marketing purposes. *See id*. Verio, in violation of these terms of service, used a "robot" program to mine Register.com's WHOIS database for contact information of customers who registered domains, and then sent

unsolicited marketing material to them. *Id*. at 245. The district court, in addressing a claim by Register.com under Section 1030(a)(2)(C) for Verio's misuse of the information it obtained from the WHOIS database, held that "even if Verio's means of access to the WHOIS database would otherwise be authorized, that access would be rendered unauthorized *ab initio* by virtue of the fact that prior to entry Verio *knows that the data obtained will be later used for an unauthorized purpose.*" *Id*. at 253 (emphasis added).

The Government respectfully submits that the latter line of cases – and not those relied on by the defendant – is better reasoned. Employers regularly grant their employees authorization to access the employer's computer systems for limited purposes, limiting access to and use of confidential business information in the employees' work. But no sane employer would grant its employees authorization to steal or otherwise misuse its confidential information. When the employer makes this understanding explicit in some manner, such as through a confidentiality agreement or confidentiality policies, there can be no question that everyone understands – the employer and the employee – that the employee has no authorization to access the employer's computers for the improper purpose of converting the confidential information to the employee's own use. In that circumstance, any authorization the employee had to access the

information would be voided if the employee knew, at the time he accessed the information, that he was going to use it for an unauthorized purpose. *See Register.com*, 126 F. Supp. 2d at 253; *Calyon*, No. 07 Civ. 2241 (RO), 2007 WL 2618658, at *1 ("[T]he plain language of the statute seems to contemplate that, whatever else, 'without access' and 'exceeds authorized access' would include an employee who is accessing documents on a computer system which that employee had to know was in contravention of the wishes and interests of his employer.").

Contrary to what the defendant and some courts claim, the Government's position here does not seek to turn every breach of a confidentiality agreement into a felony offense. Rather, the CFAA needs to be read in its entirety, including the penalty provisions. Without one of three statutory enhancements, a violation of Section 1030(a)(2)(C) is merely a misdemeanor. 18 U.S.C. § 1030(c)(2)(A). However, as is the case here, where there exists certain aggravating factors, such as when the value of information taken is greater than $5,000, the defendant seeks commercial advantage or private financial gain, or the offense is committed to aid in the commission of another crime, then 1030(c)(2)(A) is a felony. *Id*. § 1030(c)(2)(B)(i)-(iii).

In this case, the defendant was placed on notice by Goldman that (i) he was to keep "in strict confidence" Goldman's proprietary information and only use it for Goldman's business

purposes and (ii) the defendant was not authorized to transfer the source code out of Goldman's system to his home computers. The defendant was also aware that Goldman maintained various security measures which blocked certain types of transfers out of Goldman's computer system.[19] Rather than use his access to the Trading System's source code for its "intended purpose" – to improve the source code for Goldman – the defendant used his access to the system to do something he clearly did not have authorization to do, which is to transfer the source code to his home computer. Thus, like the defendant in *Morris*, the defendant here "found a hole . . . that permitted him a special and unauthorized access" the Trading System's source code. 928 F.2d at 510. In fact, the defendant admitted that he lacked authorization to transfer the code, informing the agents in his post arrest statement, in substance and in part, that he deleted records of the transfer because knew the transfer was not authorized by Goldman. That the defendant transferred the source code at the very end of his last day of work shows that there could be no legitimate Goldman-related business purpose for the transfer. Accordingly, on the facts presented here, it is clear

[19]The defendant was certainly aware of the restrictions placed on the use and transfer of the Trading System's source code, as he had to (i) identify an outside server that was not blocked by Goldman's security protocols, (ii) craft a means of transferring portions of the source code to that server, and (iii) hide evidence of the upload by deleting certain logs and programs on his Goldman computer.

that the defendant accessed the source code without authorization – and also exceeded the authorization he did have to obtain the source code for his personal use – in transferring the code from Goldman's system to his home computer.

Accordingly, the defendant's motion to dismiss Count Three should be denied.

CONCLUSION

For the foregoing reasons, the Government respectfully submits that the Defendant's Motion to Dismiss should be denied in its entirety.

Dated: July 30, 2010
New York, New York

Respectfully submitted,

PREET BHARARA
United States Attorney

/s/ J.P.F.
By:_____
Joseph P. Facciponti
Rebecca A. Rohr
Assistant United States Attorneys
Tel: (212) 637-2522/22531
Fax: (212) 637-2620